Remarks

This paper is responsive to a non-final Office action mailed May 21, 2004. A request for the necessary extension of time in which to respond is filed concurrently with this paper.

The action contains a rejection under 35 USC 103(a) of original claims 1-20 and 23-25 over US patent 6,226,750 - Trieger (hereafter *Trieger)* in view of US patent 5,751,812 - Anderson (hereafter *Anderson*).

The Office action does not include an explicit statutory rejection of original claim 26, which depends from rejected claim 25. For purposes of this response, it will be assumed that the Office's intent was to include claim 26 with all other claims rejected under 35 USC 103(a) over *Trieger* in view of *Anderson.*

The set of rejected claims includes five independent claims, each of which has a number of dependent claims. Independent claim 1 is directed to a method of controlling a plurality of separate electronic communications between first and second parties. Independent claim 7 is directed to a secure electronic communications system having means for controlling a plurality of separate electronic communications between first and second parties. Independent claim 12 is directed to a computer program having instructions which, when executed on a computer carry out a method of controlling a plurality of separate electronic communications between first and second parties. Independent claim 18 is directed to a client computer connectable for secure communication with a server computer. Independent claim 24 is directed to a server computer connectable for secure communication with one or more client computers.

Regardless of the environment defined by the independent claims, the claims share common elements. One of those elements is that both the server and client computers in a system are provided with a seed value, a mathematical advance function and a one-way hash function. When communications are to be established (or re-established) following the provision of the seed value and the mathematical advance and one-way hash functions, the computers provided this information use the mathematical advance function to create a new seed value. The one-way hash

function is applied to the new seed value to create a new security code. The new security code is sent by the client computer to the server computer, which is then compared to the new security code generated within the server computer. If the client-generated security code matches the server-generated security code, secure communications between client and server are enabled.

The Office position on the teachings of *Trieger* is a little confusing. According the action (beginning on Page 3), the *Trieger* specification teaches exchanging a seed value, a mathematical advance function and a one-way hash function in material found in Column 7 line 48 - Colum 8 line 30 and Column 10 lines 42-56. However, on Page 4, the action then states:

> *"Trieger does not explicitly disclose exchanging a seed value, a mathematical advance function and exchanging a one-way hash function."*

The position stated in the quote above is the correct one. *Trieger* clearly does not disclose or suggest exchanging a seed value, a mathematical advance function or a one-way hash function.

What *Trieger* does disclose is a session tracking technique in which client-server communications are established when the client provides a password that the server recognizes. Once the communications are established, the server generates a session-identifying key that is transmitted back to the client. The client uses the server-provided key in making transmitting subsequent requests relating to the identified session. Note that the client does not participate in any way in generating the session-identifying key. Note also that the *Trieger* invention does not relate to user authentication.

The action attempts to overcome the clear deficiencies of *Trieger* by citing *Anderson* as supposedly teaching a re-initialization function that purported shows initial exchanges of a seed value, a mathematical advance function and a one-way hash function and then subsequent use of the seed value and mathematical advance function to create a new seed value that is hashed with the one-way hash function.

Anderson is more relevant to the present invention than *Trieger* but does not teach what the Office action says it teaches. What *Anderson* does teach is the creation of login series which

permit a client user to use the same password only for a finite number of logins before changing the password.

Both the client and the server in an *Anderson* system begin with the same seed, the same password and the same hash function, which means that those parameters obviously are exchanged between the client and server. In the *Anderson* system, apparently both the client and the server establish in initial value representing *i* iterations of the hash function applied to a password *A* and a seed value *S*. On each subsequent login, the client and server apparently both calculate a hash value based on *i-1* iterations applied to the same password and seed value. The password remains valid until the number of remaining iterations is reduced to zero.

The client user must then establish a new login series by establishing a new password B based on the original seed value.

Note that *Anderson* teaches repeated use of the same seed value on successive logins. Conversely, *Anderson* does not teach the generation of new seed values for successive attempts to re-initialize communictions, which is a significant element in each of the rejected claims. *Anderson* is silent about a mathematical advance function, another significant element in each of the rejected claims. That isn't surprising. Because *Anderson* doesn't change the seed value, it has no need for a mathematical advance function.

To net out the above, neither *Trieger* nor *Anderson* teaches exchanging a seed value, a mathematical advance function and a one-way hash function and then the subsequent use of the matchematical advance function to change the seed value.

Even if *Anderson* did disclose these things, the proposed combination of the two references to incorporate the *Anderson* teachings into the *Trieger* system would still be improper since the motivation of the combination does not appear in either of the cited references. *Trieger* deals with session tracking. *Anderson* deals with communications re-initialization. There is nothing in *Trieger* that provides a motive to incorporate the cummunications re-initialization teachings of *Anderson*. There is nothing in *Anderson* to suggest why its teachings should be imported into the session tracking technology taught by *Trieger*.

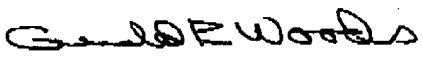
The above discussion is based on the independent claims rejected over *Trieger* and *Anderson*. Claims dependent upon those independent claims are allowable for at least the same reasons as the independent claims.

The rejection of claims 1-20 and 23-26 over the hypothetical combination of *Trieger* and *Anderson* is clearly improper and should be withdrawn.

Claims 21 and 22 were rejected under 35 USC 103(a) over the hypothetical combination of *Trieger* and *Anderson* in further view of US patent 6,338,140 - Owens. Claims 21 and 22 are dependent upon independent claim 18 and are allowable for at least the same reasons as that claim.

It is submitted that all claims in this application distinguish patentbly over the art of record and that the application is otherwise in condition for allowance.

Respectfully Submitted,



Gerald R. Woods, Reg. No. 24,144
Attorney of Record

IBM Corporation
T81/503
PO Box 12195
Research Triangle Park, NC 27709
919-(919) 543 - 7204
FAX 919-254-4330